(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Offenlegungsschrift**

(10) **DE 100 48 553 A 1**

(51) Int. Cl.[7]:
H 04 L 9/10
G 09 C 1/10

(21) Aktenzeichen: 100 48 553.7
(22) Anmeldetag: 30. 9. 2000
(43) Offenlegungstag: 18. 4. 2002

DE 100 48 553 A 1

(71) Anmelder:
Biodata Information Technology AG, 35104 Lichtenfels, DE

(74) Vertreter:
Kestler und Kollegen, 60323 Frankfurt

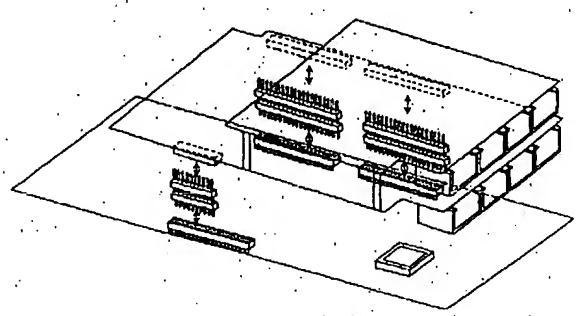
(72) Erfinder:
Antrag auf Nichtnennung

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Modularer Aufbau eines Gerätes zur Verschlüsselung von Kommunikationsdaten

(57) Das Kommunikations-Verschlüsselungsgerät Babylon-META ist modular aufgebaut. Es besteht aus einem Motherboard, auf dem sich im wesentlichen der Prozessor, Chips zur Verschlüsselung der Daten, ein SRAM zum Speichern der am Verschlüsselungsgerät vorgenommenen Einstellungen, ein Flash-EEPROM mit der Firmware, eine Schnittstelle zur Konfiguration des Gerätes, eine Real Time Clock und die optischen Anzeigeelemente des Gerätes befinden. Auf das Motherboard können verschiedene Platinen (Aufsteckmodule) mit jeweils unterschiedlichen Schnittstellen aufgesteckt werden. Dadurch wird eine Erweiterung bzw. Umrüstung des Gerätes ermöglicht, so daß eine Nutzung unterschiedlicher Schnittstellen-Varianten mit einem Gerät möglich sind.



DE 100 48 553 A 1

BUNDESDRUCKEREI 02.02 102 160/379/1

Beschreibung

[0001] Die Erfindung betrifft ein Gerät zur Verschlüsselung von Telekommunikationsdaten, die in Netzen z. B. per Telefon, Fax, PC oder Videokonferenz übertragen werden. Es handelt sich dabei um ein Gerät, das zur Verschlüsselung der zu übertragenden Daten zwischen dem entsprechenden Datenendgerät und einem Anschluß eines öffentlichen bzw. privaten Netzes angeschlossen wird. Die Gegenseite muß ebenfalls über ein solches Gerät verfügen, um die verschlüsselten Daten wiederum entschlüsseln zu können.

[0002] Innerhalb vieler Unternehmen erfolgt der Austausch von Daten fast ausschließlich digital, z. B. per Telefon, Fax, Intranet, E-Mail etc. Da die Übertragung dieser Daten vielfältige Angriffspunkte zur Wirtschaftsspionage und Datenraub bietet, gewinnen Verschlüsselungsgeräte für digitale Kommunikation immer mehr an Bedeutung. Nach dem derzeitigen Stand der Technik verfügen die Verschlüsselungsgeräte über fest installierte Schnittstellen, die für ein bestimmtes Netzwerkprotokoll vorgesehen sind. Soll die Datenübertragung auf ein anderes Netzwerkprotokoll umgestellt werden, so ist dafür der Austausch des kompletten Verschlüsselungsgerätes notwendig.

[0003] Ziel der vorliegenden Erfindung ist es, ein Verschlüsselungsgerät so zu gestalten, daß ein Wechsel auf andere Netzwerkprotokolle beim Übergang auf neue Netzwerktechnologien ohne Austausch des kompletten Verschlüsselungsgerätes möglich ist, was sich für den Kunden kostengünstig auswirkt.

[0004] Erfindungsgemäß wird dieses Ziel dadurch erreicht, daß das Motherboard des Verschlüsselungsgerätes so konstruiert ist, daß ein Aufsteckmodul mit den jeweils gewünschten Schnittstellen auf das Motherboard aufgesteckt werden kann. Mit der zugehörigen Firmware, die in das auf dem Motherboard befindliche Flash-EEPROM geladen wird, läßt sich der Wechsel auf ein anderes Netzwerkprotokoll somit leicht vollziehen. Auf dem erfindungsgemäß gestalteten Motherboard des Verschlüsselungsgerätes befinden sich drei zweireihige Buchsenleisten mit zweimal 20 Kontakten, über die die elektrische Verbindung zum jeweiligen Aufsteckmodul hergestellt wird. Auf den jeweiligen Aufsteckmodulen mit den dem gewünschten Netzwerkprotokoll entsprechenden Schnittstellen befinden sich zur Herstellung der elektrischen Verbindung zwischen Motherboard und Aufsteckmodul ebenfalls drei Buchsenleisten mit zweimal 20 Kontakten (Bussystem). Die elektrische Verbindung zwischen Motherboard und Aufsteckmodul wird dann erfindungsgemäß durch dieses Bussystem hergestellt. Die Ansteuerung der Schnittstellen auf dem Aufsteckmodul erfolgt durch die zugehörige Firmware, die sich im Flash-EEPROM auf dem Motherboard befindet. Die Anzahl der elektrischen Kontakte, die mittels der zweireihigen Stiftleisten hergestellt werden, ist abhängig vom jeweiligen Aufsteckmodul.

[0005] Die Erfindung wird nachfolgend beispielhaft für einige Aufsteckmodule anhand diverser Zeichnungen näher erläutert.

[0006] In **Fig.** 1 ist das Motherboard des Verschlüsselungsgerätes BabylonMETA mit den drei zweireihigen Buchsenleisten, über die die Verbindung zum jeweiligen Aufsteckmodul hergestellt wird, abgebildet.

[0007] **Fig.** 2 stellt ein Aufsteckmodul mit vier S0-Schnittstellenpaaren dar, darauf sind im wesentlichen die vier S0-Schnittstellen und die drei zweireihigen Buchsenleisten zur Herstellung der elektrischen Verbindung zwischen Motherboard und Aufsteckmodul erkennbar.

[0008] In **Fig.** 3 ist eine zweireihige Stiftleiste abgebildet, die das jeweilige Aufsteckmodul mit dem Motherboard des

Verschlüsselungsgerätes verbindet. Die Anzahl der Kontakte ist dabei abhängig von der Art der Aufsteckplatine.

[0009] **Fig.** 4 zeigt beispielhaft, wie ein Modul mit den benötigten Schnittstellen mit Hilfe zweireihiger Stiftleisten auf das Motherboard des Verschlüsselungsgerätes aufgesteckt wird. Das Beispiel zeigt ein Modul mit vier S0-Schnittstellenpaaren.

[0010] In **Fig.** 5 und 6 werden weitere derzeit verfügbare Aufsteckmodule abgebildet, deren Sortiment durch Neuentwicklungen jederzeit erweiterbar ist.

[0011] In der **Fig.** 1 ist das Motherboard des modular aufgebauten Verschlüsselungsgerätes abgebildet. Darauf sind im wesentlichen der Prozessor (**4**), die Chips (**6**) zur Verschlüsselung der Telekommunikationsdaten, das SRAM (**7**) zur Speicherung der am Gerät vorgenommenen Einstellungen (Konfiguration), das Flash-EEPROM (**5**) mit der zum jeweiligen Aufsteckmodul gehörigen Firmware und die zweireihigen Buchsenleisten (**1**), (**2**) und (**3**) zur Herstellung der elektrischen Verbindung zwischen dem Motherboard und dem jeweiligen Aufsteckmodul abgebildet. **Fig.** 2 zeigt beispielhaft ein Aufsteckmodul mit vier S0-Schnittstellen (**8**) und den zugehörigen zweireihigen Buchsenleisten (**9**), (**10**) und (**11**) zur Herstellung der elektrischen Verbindung mit dem Motherboard des Verschlüsselungsgerätes. Um nun ein mit den gewünschten Schnittstellen versehenes Aufsteckmodul mit dem Motherboard zu verbinden, wird mittels mehrerer in wie **Fig.** 3 dargestellten zweireihigen Stiftleisten zwischen dem Motherboard und der Aufsteckplatine ein elektrischer Kontakt hergestellt. Dadurch ist es möglich, die auf der Aufsteckplatine befindlichen Schnittstellen mit Hilfe der im Flash-EEPROM des Motherboards befindlichen und auf das zugehörige Übertragungsprotokoll abgestimmten Firmware anzusteuern.

[0012] In **Fig.** 4 wird verdeutlicht, wie ein Aufsteckmodul mit vier S0-Schnittstellen mit Hilfe von zwei zweireihigen Stiftleisten mit jeweils 2 × 20 Kontakten (**12**) und einer mit 2 × 10 Kontakten (**13**) über die auf Motherboard und Aufsteckmodul befindlichen Buchsenleisten elektrisch verbunden wird. Wieviele Kontakte zum Herstellen der elektrischen Verbindung jeweils benötigt werden, variiert von Modul zu Modul. Beispielsweise erfolgt das Aufstecken eines Moduls mit einer S2M-Schnittstelle analog zum Modul mit vier S0-Schnittstellenpaaren, während für ein Modul mit einem seriellen Schnittstellenpaar drei Stiftleisten mit 2 × 20 Kontakten benötigt werden. Die **Fig.** 5 und 6 zeigen die zusätzlich zum Modul mit vier S0-Schnittstellenpaaren momentan für das BabylonMETA verfügbaren Aufsteckmodule. **Fig.** 5 zeigt das Modul mit einem S2M-Schnittstellenpaar (**14**) und **Fig.** 6 stellt ein Aufsteckmodul mit einem seriellen Schnittstellenpaar (**15**) dar.

Patentansprüche

Modularer Aufbau eines Gerätes zur Verschlüsselung von Telekommunikationsdaten, **dadurch gekennzeichnet**, daß das Motherboard des Verschlüsselungsgerätes mit unterschiedlichen Aufsteckmodulen für verschiedene Schnittstellen kombiniert werden kann, so daß die Verschlüsselung bzw. Übertragung der Telekommunikationsdaten über verschiedene Netzwerkprotokolle mit einem Verschlüsselungsgerät möglich ist.

Hierzu 3 Seite(n) Zeichnungen

- Leerseite -

Nummer: DE 100 48 553 A1
Int. Cl.[7]: H 04 L 9/10
Offenlegungstag: 18. April 2002

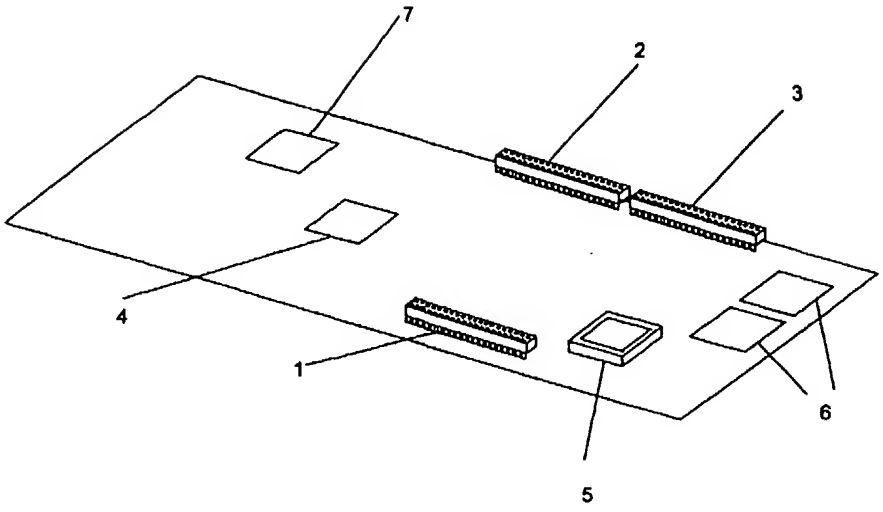


Fig. 1

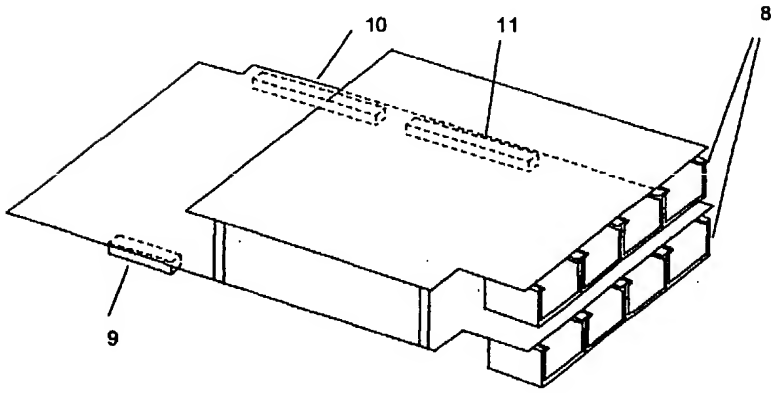


Fig. 2

Nummer: DE 100 48 553 A1
Int. Cl.[7]: H04L 9/10
Offenlegungstag: 18. April 2002

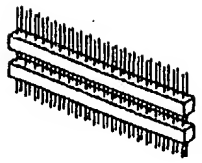


Fig. 3

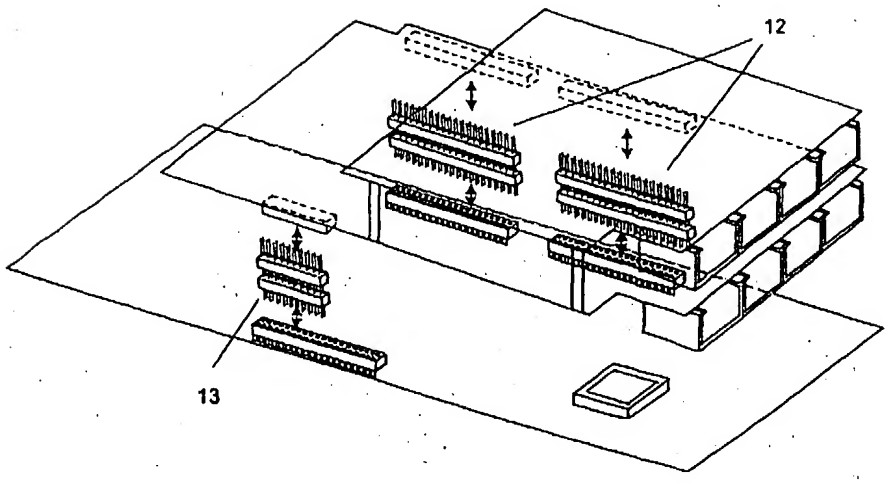


Fig. 4

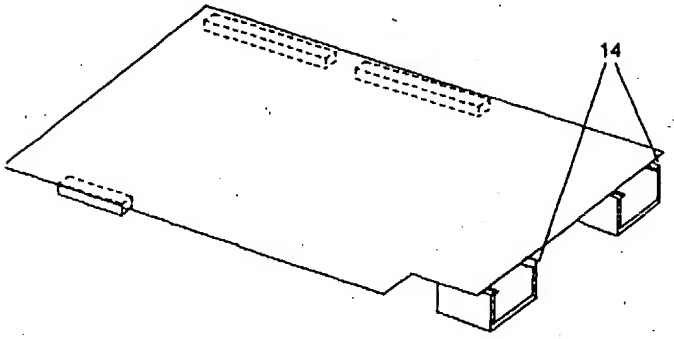


Fig. 5

Nummer: DE 100 48 553 A1
Int. Cl.[7]: H 04 L 9/10
Offenlegungstag: 18. April 2002

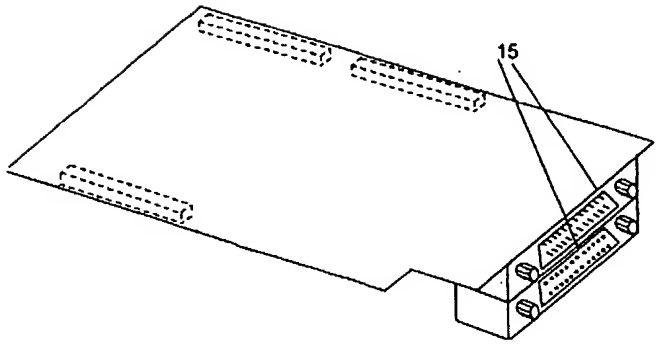


Fig. 6